

Solvable primitive extensions

Chandan Singh Dalawat
Harish-Chandra Research Institute
Chhatnag Road, Jhansi, Allahabad 211019, India
dalawat@gmail.com

Abstract. A finite separable extension E of a field F is called primitive if there are no intermediate extensions. It is called a solvable extension if the group $\text{Gal}(\hat{E}|F)$ of F -automorphisms of its galoisian closure \hat{E} over F is solvable. We show that a solvable primitive extension E of F is uniquely determined (up to F -isomorphism) by \hat{E} and characterise the extensions D of F such that $D = \hat{E}$ for some solvable primitive extension E of F .

(1) Let F be a field. All extensions of F appearing below are assumed to be *separable* over F . A finite extension E of F of degree $[E : F] > 1$ is called *primitive* if the only intermediate fields $F \subset K \subset E$ are $K = F$ and $K = E$. We say that E is *solvable* over F if the group $G = \text{Gal}(\hat{E}|F)$ is solvable, where \hat{E} is the galoisian closure of E over F . Galois proved (see below) that if E is a solvable primitive extension of F , then $[E : F] = l^n$ for some prime l and some $n > 0$. So we will later fix the prime l and the integer n as well ; extensions whose degree is a power of l will simply be called *l -extensions*. The problem is to *parametrise all solvable primitive extensions of degree l^n over F* .

(2) Let Ω be a finite set with $\text{Card}(\Omega) > 1$. A partition $(\Omega_i)_{i \in I}$ of Ω will be called *essential* if $\text{Card}(I) > 1$, $\text{Card}(\Omega_i) > 0$ for all $i \in I$ and $\text{Card}(\Omega_i) > 1$ for some $i \in I$. Let G be a subgroup of the symmetric group \mathfrak{S}_Ω . A partition $(\Omega_i)_{i \in I}$ of Ω will be called *G -stable* if G permutes the parts : if there is a map $\pi : G \rightarrow \mathfrak{S}_I$ such that $g.\Omega_i = \Omega_{\pi(g)(i)}$ for every $g \in G$ and every $i \in I$; if so, π is a homomorphism of groups. A subgroup $G \subset \mathfrak{S}_\Omega$ is called *primitive* if its order is > 1 , and no G -stable essential partition of Ω exists. Every primitive subgroup of \mathfrak{S}_Ω is transitive.

MSC2010 : Primary 12F10, 12G05, Secondary 20B15, 20C05

Keywords : Solvable extensions, primitive extensions, p -extensions

(3) (Galois) *If G is a solvable primitive subgroup of \mathfrak{S}_Ω , then there is a unique structure on Ω of an affine n -space over \mathbf{F}_l (for some prime l and some $n > 0$) such that*

$$N \subset G \subset \mathbf{AGL}(\Omega) \subset \mathfrak{S}_\Omega,$$

where N (resp. $\mathbf{AGL}(\Omega)$) is the space of translations (resp. the group of automorphisms or invertible affine maps) of the affine space Ω .

Proof. The group G is not trivial by hypothesis. Let N be a minimal normal subgroup of G . Since G is solvable, N is a vector n -space over \mathbf{F}_l for some prime l and some $n > 0$. Since G is primitive, N is transitive. Since N is commutative and transitive, Ω is an N -torsor (an affine space over \mathbf{F}_l whose space of translations is N). Finally, one checks that G acts on Ω by affine maps (because the conjugation action of G/N on N is by \mathbf{F}_l -linear maps, automatically). For more details and some historical remarks, see [2, p. 435] or [11, p. 420]. \square

(4) *Let Ω be an affine space over \mathbf{F}_l of dimension $n > 0$ and let N be its space of translations. An intermediate group $N \subset G \subset \mathbf{AGL}(\Omega)$ is solvable (resp. primitive) if and only if G/N is solvable (resp. the $\mathbf{F}_l[G/N]$ -module N is simple).*

Proof. The bit about solvability is clear. Suppose that G is imprimitive, and let $(\Omega_i)_{i \in I}$ be a G -stable essential partition of Ω (2). Since G is transitive (even N is transitive), the parts Ω_i have the same cardinal l^m , for some $m \in [1, n[$. One checks that they are affine subspaces, all parallel to each other. Their common direction $M \subset N$ is a G -stable subspace of dimension m , so N is not simple as an $\mathbf{F}_l[G/N]$ -module. Conversely, if the $\mathbf{F}_l[G/N]$ -module N is not simple, let $M \subset N$ be a G -stable subspace of some dimension $m \in [1, n[$. The family of affine subspaces of Ω of direction M is a G -stable essential partition of Ω , so G is imprimitive. For more details, see [2, p. 436]. \square

(5) *A finite extension E of F is primitive (1) if and only if the group $G = \text{Gal}(\hat{E}|F)$ is a primitive subgroup (2) of \mathfrak{S}_Ω , where $\Omega = \text{Hom}_F(E, \hat{E})$.*

Proof. Note first that G is a transitive subgroup of \mathfrak{S}_Ω . Clearly the extension E is primitive over F if and only if the subgroup $H = \text{Gal}(\hat{E}|E)$ is maximal in G . Now, H is the stabiliser of $j_E \in \Omega$, where j_E is the inclusion of E in \hat{E} , and stabilisers of points are maximal subgroups if and only if the transitive permutation group is primitive. \square

(6) *If E is a solvable primitive extension of F , then $[E : F] = l^n$ for some prime l and some $n > 0$.*

Proof. Since $G = \text{Gal}(\hat{E}|F)$ is a solvable by definition (1) and primitive (5) as a subgroup of \mathfrak{S}_Ω ($\Omega = \text{Hom}_F(E, \hat{E})$), one has $\text{Card } \Omega = l^n$ for some prime l and some $n > 0$ (3). But $[E : F] = \text{Card } \Omega$, hence the result. \square

(7) This being so, let us fix the prime l and the integer $n > 0$, and parametrise the set of solvable primitive extensions E of F of degree l^n . We will show that E is determined (up to F -isomorphism) by its galoisian closure \hat{E} , and characterise the galoisian extensions of F which arise in this way, thereby establishing a canonical bijection between the set of such E and the set of certain pairs (ρ, D) which we now describe. Basically, the pair we attach to E is a way of encapsulating the information carried by \hat{E} , so let us begin by making that information explicit.

(8) We have seen (3) that the minimal normal subgroup N of $\text{Gal}(\hat{E}|F)$ is an \mathbf{F}_l -space of dimension n , and it is a faithful simple module (4) over $\text{Gal}(K|F)$, where $K = \hat{E}^N$. Denote by ρ this representation of $\text{Gal}(K|F)$ on N . As $\text{Gal}(K|F)$ is a quotient of $\text{Gal}(\tilde{F}|F)$, where \tilde{F} is a maximal galoisian extension of the field F , ρ can be viewed as a representation of $\text{Gal}(\tilde{F}|F)$; we then have $K = \tilde{F}^{\text{Ker } \rho}$. So from E we get the pair (ρ, \hat{E}) consisting of an irreducible \mathbf{F}_l -representation ρ of $\text{Gal}(\tilde{F}|F)$ of degree n with solvable image, and an elementary abelian l -extension (namely \hat{E}) of the fixed field K of the kernel of ρ which is galoisian over F and such that the conjugation action of $\text{Gal}(K|F)$ on $N = \text{Gal}(\hat{E}|K)$ resulting from the short exact sequence $1 \rightarrow N \rightarrow \text{Gal}(\hat{E}|F) \rightarrow \text{Gal}(K|F) \rightarrow 1$ is given by ρ .

(9) Conversely, suppose that we are given a pair (ρ, D) consisting of an irreducible representation ρ of $\text{Gal}(\tilde{F}|F)$ on some \mathbf{F}_l -space N of dimension n with solvable image, and an N -extension D of the fixed field K of the kernel of ρ such that D is galoisian over F and such that the resulting conjugation action of $\text{Gal}(K|F)$ on $N = \text{Gal}(D|K)$ is given by ρ . We will show that such a pair (ρ, D) determines a solvable primitive extension E of F of degree l^n , unique up to F -isomorphism, such that the pair associated to E by the construction (8) is (ρ, D) . This will establish the desired canonical bijection between the set of such E and the set of such pairs (ρ, D) . The point of having such a bijection is that for certain fields F , the pairs (ρ, D) can be explicitly computed, as is explained briefly in (18). Let's get going.

(10) *Let G be a finite group and M an $\mathbf{F}_l[G]$ -module. If G is solvable and M is faithful and simple, then $H^i(G, M) = \{0\}$ for every $i > 0$.*

Proof (Jeremy Rickard [12]). This is clear if the group G is trivial (in which case $M = \mathbf{F}_l$), so assume that the order of G is > 1 (so that $M \neq \mathbf{F}_l$). Let N be a minimal normal subgroup of G . Since G is solvable, N is an \mathbf{F}_p -

space (for some prime p) of some dimension $a > 0$. By Clifford's theorem (the restriction of an irreducible representation to a normal subgroup is semisimple) [1], the $\mathbf{F}_l[N]$ -module M is semisimple.

If we had $p = l$, the $\mathbf{F}_l[N]$ -module M would be trivial, contradicting the faithfulness of the G -module M . So $p \neq l$. Consider the central idempotent $r_N = p^{-a} \sum_{n \in N} n$ of $\mathbf{F}_l[G]$, and put $s_N = 1 - r_N$. Clearly, we have a *direct sum* decomposition as an $\mathbf{F}_l[G]$ -module : $M = r_N M + s_N M$. Since M is simple, we must have $M = r_N M$ or $M = s_N M$.

If we had $M = r_N M$, the action of N on M would be trivial (since the only simple $\mathbf{F}_l[N]$ -module which is not killed by r_N is \mathbf{F}_l), again contradicting the faithfulness of the G -module M . Therefore $M = s_N M$, which implies that M and the trivial module \mathbf{F}_l are in different blocks of $\mathbf{F}_l[G]$ (whatever that may mean), and hence $H^i(G, M) = \text{Ext}_{\mathbf{F}_l[G]}^i(\mathbf{F}_l, M) = \{0\}$ for every $i > 0$. C'est gagné ! \square

(11) *Let G be a finite solvable group and let M be a faithful simple $\mathbf{F}_l[G]$ -module. Every extension L of G by the G -module M (any short exact sequence $\{1\} \rightarrow M \rightarrow L \rightarrow G \rightarrow \{1\}$ in which the conjugation action of G on M is the given module structure) splits, and any two sections $G \rightarrow L$ are conjugate in L .*

Proof. This follows from the case $i = 2$ (resp. $i = 1$) of (10). Indeed, extensions of G by the G -module M are classified by the group $H^2(G, M)$, and we have seen that this group is trivial. Similarly, conjugacy classes of sections of the split extension of G by M are classified by the group $H^1(G, M)$, and this group too has been shown to be trivial. \square

(12) *Remark.* See [12] for a direct proof that in a solvable primitive permutation group L with minimal normal subgroup M (an \mathbf{F}_l -space), there is a unique conjugacy class of complements to M (all of them maximal subgroups, since each is the stabiliser of a point). I thank Peter Neumann for pointing out that this is covered in the books by Doerk & Hawkes (p. 55), Huppert I (p. 159), and Suzuki II (p. 102).

(13) *Every pair (ρ, D) as in (9) comes, via the construction (8), from a unique solvable primitive extension E of F of degree l^n .*

Proof. Let $K = \tilde{F}^{\text{Ker } \rho}$ be the fixed field of the kernel of ρ . We have seen that the short exact sequence

$$1 \rightarrow \text{Gal}(D|K) \rightarrow \text{Gal}(D|F) \rightarrow \text{Gal}(K|F) \rightarrow 1$$

splits and any two sections are conjugate (11), so there is an extension E of F (unique up to F -isomorphism) linearly disjoint from K and such that

$\hat{E} = EK = D$. Since the group $\text{Gal}(D|F)$ is solvable and primitive (4), and the minimal normal subgroup $\text{Gal}(D|K)$ is an \mathbf{F}_l -space of dimension n , the extension E of F is solvable and primitive (5) of degree l^n . \square

(14) **Summary.** A solvable primitive l -extension E of F is uniquely determined (up to F -isomorphism) by its galoisian closure \hat{E} over F . A galoisian extension D of F is of the form \hat{E} for some solvable primitive l -extension E of F if and only if D is an elementary abelian l -extension of the fixed field K of the kernel of an irreducible \mathbf{F}_l -representation ρ of $\text{Gal}(\tilde{F}|F)$ with solvable image such that D is galoisian over F and the resulting conjugation action of $\text{Gal}(K|F)$ on $\text{Gal}(D|K)$ is given by ρ . In terms of the parameter (ρ, D) of E , the group $\text{Gal}(\hat{E}|F)$ is given by $\text{Gal}(D|K) \times_{\rho} \text{Gal}(K|F)$.

This parametrisation is useful when F is a p -field (a local field with finite residue field of characteristic p) because we can classify irreducible \mathbf{F}_l -representations ρ of $\text{Gal}(\tilde{F}|F)$ and, for every such ρ , determine the structure of the $\mathbf{F}_l[\text{Gal}(K|F)]$ -module $\text{Gal}(M|K)$, where K is the fixed field of the kernel of ρ and M is the maximal abelian extension of K of exponent l . See (18) for a brief discussion.

(15) **Primitive quartic extensions.** Taking $l = 2$ and $n = 2$, one can parametrise primitive quartic extensions (solvability is automatic because \mathfrak{S}_4 is solvable). The action of $\mathbf{GL}_2(\mathbf{F}_2)$ on the set $\mathbf{P}_1(\mathbf{F}_2)$ consisting of the three lines in \mathbf{F}_2^2 identifies it with \mathfrak{S}_3 . With this identification, the only subgroups for which \mathbf{F}_2^2 is a simple module are \mathfrak{A}_3 and \mathfrak{S}_3 ; denote these irreducible representations by a_3 and s_3 respectively. So there are two kinds of primitive quartic extensions E depending upon whether the group $\text{Gal}(\hat{E}|F)$ is isomorphic to $\mathfrak{A}_4 = \mathbf{F}_2^2 \times_{a_3} \mathfrak{A}_3$ or to $\mathfrak{S}_4 = \mathbf{F}_2^2 \times_{s_3} \mathfrak{S}_3$, where \hat{E} is the galoisian closure of E over F . Conversely, given any \mathfrak{A}_4 - or \mathfrak{S}_4 -extension D , there is a unique (up to isomorphism) primitive quartic extension E such that $\hat{E} = D$.

(16) **Primitive quartic fields.** When $F = \mathbf{Q}$, class field theory can be used to determine all such D and hence all primitive quartic fields E . According to the database [9], the smallest (primitive) quartic field E with $\text{Gal}(\hat{E}|\mathbf{Q})$ isomorphic to \mathfrak{A}_4 (resp. \mathfrak{S}_4) is the one defined by $x^4 - 2x^3 + 2x^2 + 2$ (resp. $x^4 - x + 1$). In the first case, the corresponding \mathfrak{A}_3 -field is the one defined by $x^3 - x^2 - 2x + 1$, and in the second case the \mathfrak{S}_3 -field is the galoisian closure of the cubic field defined by $x^3 - 4x - 1$. I thank John Jones for confirming this information.

(17) **Primitive quartic extensions of \mathbf{Q}_2 .** Let K be the unique $(\mathbf{Z}/3\mathbf{Z})$ -extension of \mathbf{Q}_2 . It can be checked that K has a unique biquadratic extension D which is galoisian over \mathbf{Q}_2 and such that the conjugation action of $\text{Gal}(K|\mathbf{Q}_2) = \mathbf{Z}/3\mathbf{Z}$ on $\text{Gal}(D|K)$ is through a_3 (15). This D is thus the unique \mathfrak{A}_4 -extension of \mathbf{Q}_2 ; up to isomorphism, the corresponding primitive quartic extension is $\mathbf{Q}_2(x)$, where $x^4 - 2x^2 + 2x - 2 = 0$.

Now let K stand for the unique \mathfrak{S}_3 -extension of \mathbf{Q}_2 . It can be checked that K has *three* biquadratic extensions D which are galoisian over \mathbf{Q}_2 and such that the conjugation action of $\text{Gal}(K|\mathbf{Q}_2) = \mathfrak{S}_3$ on $\text{Gal}(D|K)$ is through s_3 (15). Thus there are precisely three \mathfrak{S}_4 -extensions D of \mathbf{Q}_2 . The corresponding primitive quartic extensions of \mathbf{Q}_2 are given (up to isomorphism) by

$$x^4 - 2x + 2, \quad x^4 - 4x + 2, \quad x^4 - 4x^2 + 4x - 2.$$

The four polynomials defining the four primitive quartic extensions of \mathbf{Q}_2 are taken from [10, p. 111]. Of course, one can arrive at them directly by examining all polynomials $x^4 + 2ax^3 + 2bx^2 + 2cx + 2d$ with $a, b, c \in \mathbf{Z}_2$ and $d \in \mathbf{Z}_2^\times$ (Eisenstein polynomials).

(18) **The local theory.** The main aim of this series of four Notes, of which this is the first and purely algebraic one, is to parametrise the set of (solvable) primitive l -extensions of a p -field F — a local field with finite residue field of characteristic p . This problem was already considered by Krasner in the 1930s, at least when F is a finite extension of \mathbf{Q}_p . Every finite (separable) extension of a p -field is solvable, and the case $l = p$ is the only interesting one. Thus, our final result will be a parametrisation of the set of all primitive p -extensions of p -fields. Primitive quartic extensions of \mathbf{Q}_2 discussed in (17) will turn out to be the simplest special case of the general theory.

In order to carry out the approach summarised in (14), the second paper [5] of this series determines the irreducible \mathbf{F}_p -representations ρ of $\text{Gal}(\tilde{F}|F)$, mostly following Koch. We will observe that if we fix $n > 0$, then there is a certain explicit finite tamely ramified split galoisian extension L_n of F which contains the fixed field of the kernel of every ρ of degree n (and such that, if F has characteristic 0, then L_n^\times has an element of order p).

Here, a tamely ramified galoisian extension L of F is said to be *split* if, L_0 being the maximal unramified extension of F in L , the short exact sequence

$$1 \rightarrow \text{Gal}(L|L_0) \rightarrow \text{Gal}(L|F) \rightarrow \text{Gal}(L_0|F) \rightarrow 1$$

splits. It can be shown that the splitting of this sequence is equivalent to the existence of an intermediate extension $F \subset E \subset L$ which is totally ramified (but not necessarily galoisian) over F and such that $[E : F] = [L : L_0]$. See [4, Remark 7.1.4], for example.

The elementary abelian p -extensions D of the fixed field K of the kernel of ρ which are galoisian over F and such that the resulting conjugation action of $\text{Gal}(K|F)$ on $\text{Gal}(D|K)$ is given by ρ will be understood in terms of the $\text{Gal}(L_n|F)$ -modules $L_n^\times/L_n^{\times p}$ in characteristic 0 and $L_n^+/\wp(L_n^+)$ in characteristic p , where $\wp(x) = x^p - x$. Therefore we study the filtered galoisian module $L^\times/L^{\times p}$ (resp. $L^+/\wp(L^+)$) for any finite tamely ramified split galoisian extension L of F in the third paper [6], mostly following Iwasawa in characteristic 0 and extending the results to characteristic p .

Using these three ingredients, the set of primitive extensions E of the p -field F is parametrised in the fourth and final paper [7] of this series. We show there that not only the discriminant of E but the filtered group $\text{Gal}(\hat{E}|F)$ (where \hat{E} is the galoisian closure of E over F) can be recovered from its parameter, and illustrate the theory in the simplest case of primitive quartic extensions of dyadic fields (or 2-fields). In particular, the primitive quartic extensions of \mathbf{Q}_2 (17) will be recovered without every having to write down a polynomial.

We also make some historical remarks in [7] ; suffice it to say here that this method is a vast generalisation from the case $n = 1$ treated in [3] and that similar but somewhat less precise results have recently been obtained by Del Corso, Dvornicich and Monge [8] when the p -field F has characteristic 0.

(19) **Sources.** The proof of Galois's theorem (3) is taken from Cox [2] and Neumann [11] ; both authors include detailed historical analyses. The related statement (4) is taken from [2]. Prompt and elegant answers to the MathOverflow question [12] were graciously provided by Geoff Robinson, Jeremy Rickard and Peter Neumann. I want to express here my heartfelt gratitude to them all.

BIBLIOGRAPHY

- [1] CLIFFORD (A). — *Representations induced in an invariant subgroup*, Annals of Math. **38** (1937) 3, 533–550.
- [2] COX (D). — *Galois theory*, Second edition. John Wiley & Sons, Inc., Hoboken, NJ, 2012. xxviii+570 pp.

- [3] DALAWAT (C). — *Serre’s “formule de masse” in prime degree*, Monatshefte Math. **166** (2012) 1, 73–92. Cf. arXiv:1004.2016v6.
- [4] DALAWAT (C) & LEE (JJ). — *Tame ramification and group cohomology*, J. Ramanujan Math. Soc. **32** (2017) 1, 51–74. Cf. arXiv:1305.2580v4.
- [5] DALAWAT (C). — *\mathbf{F}_p -representations over p -fields*, arXiv:1608.04181.
- [6] DALAWAT (C). — *Little galoisian modules*, arXiv:1608.04182.
- [7] DALAWAT (C). — *Wildly primitive extensions*, arXiv:1608.04183.
- [8] DEL CORSO (I), DVORNICICH (R) & MONGE (M). — *On wild extensions of a p -adic field*, J. Number Theory **174** (2017), 322–342. Cf. aXiv:1601.05939.
- [9] FONCTION (L). — *The L-functions and modular forms database*, online database, <http://www.lmfdb.org/>
- [10] HENNIART (G). — *Representations du groupe de Weil d’un corps local*, http://sites.mathdoc.fr/PMO/feuilleter.php?id=PMO_1979
- [11] NEUMANN (P). — *The concept of primitivity in group theory and the Second Memoir of Galois*, Arch. Hist. Exact Sci. **60** (2006) 4, 379–429.
- [12] OVERFLOW (M). — *Solvable irreducible subgroups of the \mathbf{GL}_n of \mathbf{F}_p (p prime)*, <http://mathoverflow.net/q/241982>